二次元符号 (群論と組み合せ論)

AUTHOR(S):

今井, 秀樹

CITATION:

今井, 秀樹. 二次元符号 (群論と組み合せ論). 数理解析研究所講究録 1973, 178: 65-78

ISSUE DATE:

1973-05

URL:

http://hdl.handle.net/2433/107103

数理解析研究所講究録
178巻 1973年 65-78

二次元符号

横浜国大・工　今井秀樹

§1. まえがき

符号理論では，これまで，符号はシンボルが一次元に配列されたものとして扱われてきた。これは従来の情報の伝達および処理が一次元的に行われてきたからであろう。しかし，将来，二次元情報の処理技術の発展に伴い，シンボルが二次元に配列された符号も必要になってくると思われる。

本稿では最近の二次元符号の研究について概説する。なお，ここでは簡単のため，シンボルが0，1からなる二元符号についてのみ論ずる。

§2. 一次元符号について

はじめに，準備として，従来の符号——一次元符号について簡単に述べておこう。符号を用いる目的は，情報をできるだけ誤りなく伝えることである。いま，図1のように，kビットの情報 $a_0, a_1, \cdots, a_{k-1}$ を送りたいとしよう。a_i は0ま

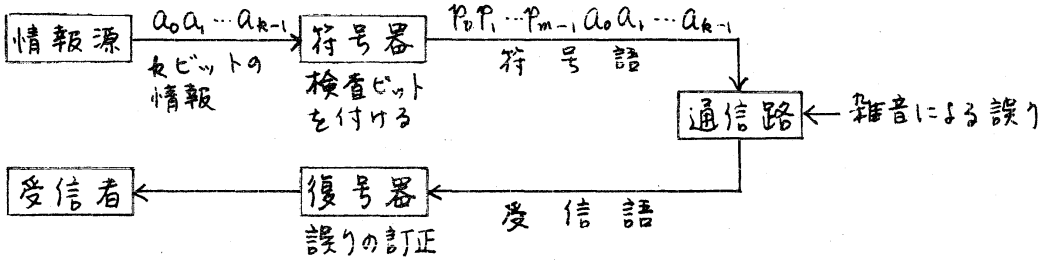

図1. 誤り訂正符号（組織符号）を用いる通信系

または1であるが、これをGF(2)の元として扱うと便利である。また、$a_0a_1\cdots a_{k-1}$としては、0, 1からなる長さkのあらゆるパターンが現れ得るとする。これをこのまま送ったのでは、通信路で誤りが生じたとき、それを訂正することができないから、信頼性を上げるためには、符号器で何らかの冗長性を付与しなければならない。そこで、情報ビット$a_0, a_1, \cdots a_{k-1}$にm個の検査ビット$p_0p_1\cdots p_{m-1}$をつけ加えて通信路に送り出すのである。これらの検査ビットは情報ビットの何らかの関数として定められる。たとえば、$k=3$, $m=4$として、検査ビットを

$$\left.\begin{aligned} p_0 &= a_0 + a_2 & p_1 &= a_0 + a_1 + a_2 \\ p_2 &= a_0 + a_1 & p_3 &= a_1 + a_2 \end{aligned}\right\} \quad (1)$$

によって定めるものとしよう。ただし、これらはGF(2)上の式である。このとき、情報ビットのあらゆるパターンに対し、通信路に送り出される系列を示すと表1のようになる。このような系列の集合が<u>符号</u>であり、各系列が<u>符号語</u>である。

この符号においては符号語の長さが有限で，しかもすべて等しい．このような符号をブロック符号という．そして，符号語の長さ $n=k+m$ を符号長という．さらに，表1の符号は，情報ビットと検査ビットを区別できるという意味で組織符号と呼ばれるものであり，また，検査ビットが情報ビットの線形関数で与えられるという意味で線形符号と呼ばれるものである．いうまでもなく，線形符号は GF(2) の上の n 次元ベクトル空間の k 次元部分空間をなす．

表1．符号長7，情報ビット数3の線形符号（巡回符号）．

検査ビット			情報ビット		
p_0	p_1	p_2	p_3	a_0	a_1	a_2
0	0	0	0	0	0	0
1	1	1	0	1	0	0
0	1	1	1	0	1	0
1	0	0	1	1	1	0
1	1	0	1	0	0	1
0	0	1	1	1	0	1
1	0	1	0	0	1	1
0	1	0	0	1	1	1

さて　表1の符号はさらに興味深い特徴をもっている．それは，符号語を $\mathbf{C}=(C_0, C_1, \cdots, C_{n-1})$ とすると，そのシンボルを巡回置換した $(C_{n-1}, C_0, C_1, \cdots, C_{n-2})$ も符号語になっているということである．このように任意の符号語の巡回置換が再び符号語となる線形符号を巡回符号と呼ぶ．巡回符号を論ずる場合には，符号語 $\mathbf{C}$ を GF(2) の上の多項式

$$C(x)=C_0+C_1x+\cdots+C_{n-1}x^{n-1} \qquad (2)$$

で表わしておくと便利である．これを符号多項式と呼ぼう．ここで，符号長 n，情報ビット数 k の巡回符号における最小次数の非零の符号多項式を $G(x)$ とおく．これは $n-k$ 次の多項式となる．そして，巡回符号のすべての符号多項式は $G(x)$ で割り切れ，また，$G(x)$ で割り切れる $n-1$ 次以下の $GF(2)$ の上の多項式は，この巡回符号の符号多項式となることが導ける．このような $G(x)$ を巡回符号の生成多項式と呼ぶ．たとえば，表1の巡回符号の生成多項式は $G(x)=1+x+x^2+x^4$ である．巡回符号は生成多項式によって完全に特徴づけられ，また，生成多項式を用いることにより，簡単なシフトレジスター回路で符号化を行えるのである．

さて，符号理論では，通信路で生じる誤りとしてランダム誤りとバースト誤りの二つの型のものを考える．ランダム誤りとは，個々の誤りが他の誤りと統計的に独立に生じる場合をいう．これに対し，バースト誤りとは，誤りの間に相関があり，密集して生じる誤りをいう．ランダム誤り訂正符号については文献に譲り，ここでは，バースト誤り訂正符号についてもう少し述べておこう．ふつう，バースト誤りの大きさを測るものとして，その長さが用いられる．バースト誤りの長さとは，最初の誤りから最後の誤りまでの長さである．たとえば，通信路で


（斜線部が誤り）

という誤りが生じたとしよう．これをバースト誤りと考えれば，長さは6である．もちろん，ランダム誤り訂正符号を用いてもバースト誤りを訂正することはできるが，誤り相互の間の相関を利用すれば，バースト誤りはより能率よく（より少数の検査ビットで）訂正できるはずである．このために，バースト誤り訂正符号が用いられるのである．

バースト誤り訂正符号としてよく知られているものに<u>ファイア符号</u>がある．これは，生成多項式が

$$G(x) = P(x)(x^c - 1) \qquad (3)$$

となる符号長 $n = LCM(e, c)$ の巡回符号である．ただし，$P(x)$ は既約多項式であり，e は $P(x)$ の根の位数である．また，c は e で割り切れない正整数とする．$P(x)$ の次数を m とすれば，この符号の検査ビット数は $c+m$ であり，長さ b が

$$b \leq m, \qquad b \leq (c+1)/2 \qquad (4)$$

を満たすバースト誤りを訂正できる．また，ファイア符号の符号化および復号はシフトレジスターを用いて容易に行える．

ところで，$n-1$ 次以下の多項式 $C(x)$ がファイア符号の符号多項式となる必要十分条件は，もちろん $C(x)$ が $G(x)$ で割り切れることであるが　これはまた，$P(x)$ の根

α ($\in GF(2^m)$) を用いて,

$$C(x) \equiv 0 \mod (x^c - 1), \quad C(\alpha) = 0 \qquad (5)$$

とかけることに注意しておこう.

以上, 一次元符号についてきわめて簡単に述べた. 詳しくは文献(1)~(5)を参照されたい.

さて, 符号理論では, 以上のような誤り訂正符号の他に, ある種の周期系列を扱うことがある. その中で代表的なものはM系列(最大長シフトレジスター系列)である. これは, 一定数の記憶素子をもつ入力のない線形シフトレジスターで発生し得る最長周期の系列であり, 記憶素子数をmとすれば, 周期は$2^m - 1$である. M系列はm次の原始多項式に対応した結線をもつ線形帰還シフトレジスターによって発生させることができる. たとえば, 原始多項式$1 + x + x^3$に対応する図2のシフトレジスターに非零の任意の初期状態を与えれば, 一周期が1110100となる周期7のM系列が発生する.

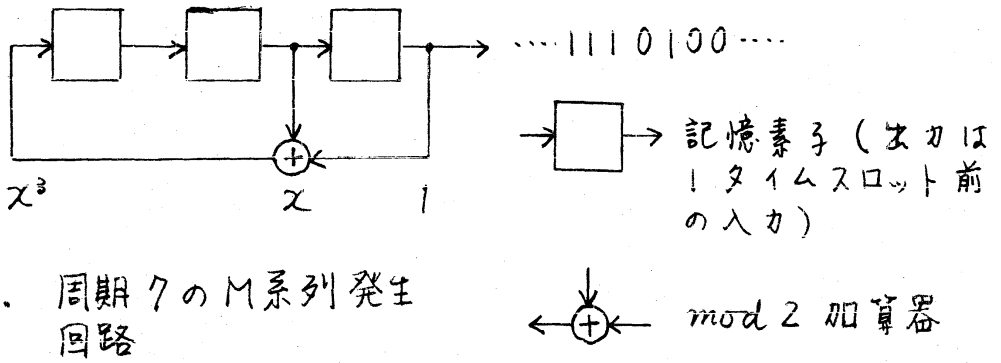

図2. 周期7のM系列発生回路

M系列はまた次のように表わすこともできる．$GF(2^m)$の原始元をαとし，θを$GF(2^m)$から$GF(2)$の上への任意の線形写像とすれば，$s_i=\theta(\alpha^i)$をi成分とする系列$\{s_i\}$は周期2^m-1のM系列となるのである．

M系列は種々の興味深い性質をもっている．その一つは自己相関関数である．いま，ηを$GF(2)$から実数への

$$\eta(0)=+1\ ,\qquad \eta(1)=-1 \tag{6}$$

という写像とし，周期nの系列$\{s_i\}$に対し，

$$\rho(k)=\left[\sum_{i=0}^{n-1}\eta(s_i)\eta(s_{i+k})\right]/n \tag{7}$$

で自己相関関数を定義すれば，M系列の自己相関関数は

$$\rho(k)=\begin{cases}1 & ;\ k=hn\ (h:\text{整数})\\ -1/n & ;\ \text{その他の場合}\end{cases} \tag{8}$$

となることが導ける．つまり，周期の整数倍のところで鋭いピークをもち，それ以外の点ではごく小さな値をとるのである．

§3. 二次元符号

これまで述べてきた符号はシンボルが一次元に配列されていた．これに対し，符号語が

$$C=\begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n_2-1}\\ c_{1,0} & c_{1,1} & \cdots & c_{1,n_2-1}\\ \vdots & \vdots & & \vdots\\ c_{n_1-1,0} & c_{n_1-1,1} & \cdots & c_{n_1-1,n_2-1}\end{bmatrix} \tag{9}$$

という形の符号を面積 $n_1 \times n_2$ の二次元符号と呼ぶ．このような二次元符号についても，線形符号は一次元符号の場合と全く同様に考えることができる．線形という性質に関する限り，一次元と二次元に本質的な差異はない．しかし，巡回性については，一次元と二次元ではやや様相を異にする．二次元巡回符号は，式(9)の C が符号語であれば，

$$\begin{bmatrix} c_{n_1-1,0} & c_{n_1-1,1} & \cdots & c_{n_1-1,n_2-1} \\ c_{0,0} & c_{0,1} & \cdots & c_{0,n_2-1} \\ \vdots & \vdots & & \vdots \\ c_{n_1-2,0} & c_{n_1-2,1} & \cdots & c_{n_1-2,n_2-1} \end{bmatrix} \text{ および } \begin{bmatrix} c_{0,n_2-1} & c_{0,0} & \cdots & c_{0,n_2-2} \\ c_{1,n_2-1} & c_{1,0} & \cdots & c_{1,n_2-2} \\ \vdots & \vdots & & \vdots \\ c_{n_1-1,n_2-1} & c_{n_1-1,0} & \cdots & c_{n_1-1,n_2-2} \end{bmatrix} \quad (10)$$

が符号語となるような二次元線形符号と定義される．この場合にも符号語を

$$C(x,y) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} c_{ij} x^i y^j \quad (11)$$

という GF(2) の上の二変数多項式で表わしておくと便利である．しかし，一般に，二次元巡回符号は，一次元巡回符号の場合のように単一の生成多項式で特徴づけることはできない．このため，二次元巡回符号の取扱いは一次元の場合よりもかなり複雑となる．たとえば，一次元巡回符号の場合，検査ビットの位置については全く問題が生じない．ところが二次元ではそうはいかない．二次元巡回符号の検査ビットの位置は符号によって様々な形をとるのである．

さて二次元面上に生じたランダム誤りを訂正しようとい

う場合には，敢えて二次元符号を使う必要はない．一次元のランダム誤り訂正符号を適当に二次元に配列し直して用いればよいからである．これに対し，二次元面上にインキのしみのように生じた二次元バースト誤りは，二次元符号を用いることにより，より能率よく訂正できる．

二次元バースト誤りの場合，一次元バースト誤りの長さに対応するものは面積である．これは，二次元面上のすべての誤りを含む最小の矩形の大きさと定義される．たとえば，図3のような誤りは面積2×3の二次元バースト誤りである．このような二次元バースト誤りを訂正する符号として代表的なものは二次元ファイア符号である．次節でこの符号について述べよう．

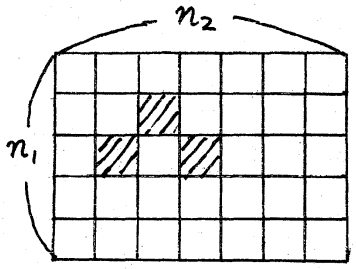

図3．面積2×3の二次元バースト誤り

§4．二次元ファイア符号

m_1, m_2 を正整数とし，α を $GF(2^{m_1 m_2})$ の原始元とする．また，e_1, e_2 を

$$e_1 e_2 = 2^{m_1 m_2} - 1 \tag{12}$$

$e_1 \mid 2^k - 1$ となる最小の正整数 $k = m_1$ (13)

$$GCD(e_1, e_2) = 1 \tag{14}$$

を満たす正整数とし，

$$\gamma = \alpha^{e_2} \qquad \beta = \alpha^{e_1} \tag{15}$$

とおく．つぎに，c_1，c_2 をその積 $c_1 c_2$ が $2^{m_1 m_2}-1$ で割り切れない正整数とし，

$$n_1 = LCM(c_1, e_1), \quad n_2 = LCM(c_2, e_2) \tag{16}$$

とおく．このとき，

$$\left.\begin{aligned} &C(x, y) \equiv 0 \mod (x^{c_1}-1,\ y^{c_2}-1) \\ &C(\gamma, \beta) = 0 \end{aligned}\right\} \tag{17}$$

を満たす x に関して n_1 次未満，y に関して n_2 次未満の GF(2) 上の多項式 $C(x, y)$ すべての集合が二次元ファイア符号である．（より一般的な定義については文献 (9) 参照.）この符号は面積 $n_1 \times n_2$ の二次元巡回符号である．そして，$c_1 c_2 + m_1 m_2$ 個の検査ビットをもち，これらは図4のような位置にとることができる．また，この符号は面積 $b_1 \times b_2$ が

$$\left.\begin{aligned} &b_1 \le (c_1+1)/2, \quad b_2 \le (c_2+1)/2 \\ &b_1 \le m_1, \qquad b_2 \le m_2 \end{aligned}\right\} \tag{18}$$

を満たす二次元バースト誤りを訂正できることが導ける．たとえば，$m_1 = m_2 = 2$ とすると，$e_1 = 3$，$e_2 = 5$ は式 (12)～(14) を満たす．いま，$c_1 = 4$，$c_2 = 3$ とすれば，面積 12×15 の二次元ファイア符号ができる．こ

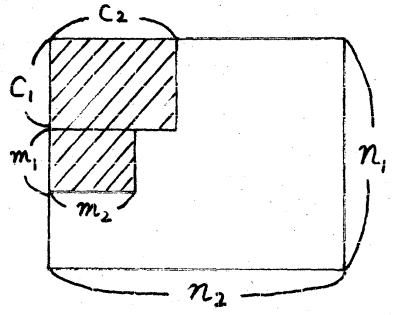

図4. 二次元ファイア符号の検査ビットの位置（$m_2 \le c_2$ とする）

の符号の検査ビット数は 16 であり，面積 2×2 以下の二次元バースト誤りを訂正できる．

二次元ファイア符号の符号化および復号は二次元に記憶素子を配列したシフトレジスターを用いて行える．詳しくは文献(9)を参照されたい．

なお，二次元バースト誤り訂正符号の他の構成法も二，三知られている(7)(8)．

§5. M平面

つぎに，二次元周期系列について考えよう．二次元系列

$$\{S_{ij}\} = \begin{array}{c} \cdots \quad \vdots \quad \cdots \quad \vdots \quad \cdots \\ \cdots\ S_{i-1,j-1}\ S_{i-1,j}\ S_{i-1,j+1}\ \cdots \\ \cdots\ S_{i,j-1}\ S_{i,j}\ S_{i,j+1}\ \cdots \\ \cdots\ S_{i+1,j-1}\ S_{i+1,j}\ S_{i+1,j+1}\ \cdots \\ \cdots \quad \vdots \quad \cdots \quad \vdots \quad \cdots \end{array} \tag{19}$$

において，すべての整数 i, j に対し，

$$S_{i+n_1,j} = S_{ij}\ , \qquad S_{i,j+n_2} = S_{ij} \tag{20}$$

を満たす最小の正整数 n_1, n_2 が存在するとき，$\{S_{ij}\}$ は周期 (n_1, n_2) の二次元周期系列であるという．二次元周期系列として重要なものはM平面である．これはM系列を二次元に拡張したもので，多くの興味深い性質をもっている．

M平面は様々な方法で定義できるが，前節式(15)の γ, β を用いて定義するのがもっとも簡単である．このことからM平面はまた $\gamma\beta$ 平面とも呼ばれる．ここで，θ を $GF(2^{m_1 m_2})$

からGF(2)の上への任意の線形写像としよう．このとき

$$s_{ij} = \theta(\gamma^i \beta^j) \qquad (21)$$

を(i, j)要素とする二次元系列$\{s_{ij}\}$がM平面となるのである．このM平面の周期は$(n_1, n_2) = (e_1, e_2)$である．

1	0	0	1	0	1	0	0	1
0	1	1	1	0	1	1	1	0
1	0	1	0	0	0	1	0	1
0	0	1	1	0	1	1	0	0
0	1	0	0	0	0	0	1	0
1	1	1	0	0	0	1	1	1
1	1	0	1	0	1	0	1	1

図5．周期(7, 9)のM平面の一周期

たとえば，$m_1 = 3$，$m_2 = 2$とすれば，$e_1 = 7$，$e_2 = 9$は式(12)～(14)を満たす．いま，αを原始多項式$1 + x + x^6$の根とし，$\theta(\gamma^i \beta^j)$を$\gamma^i \beta^j$を$\alpha^0, \alpha^1, \cdots, \alpha^5$の線形結合で表わしたときの$\alpha^0$の係数とすれば，一周期が図5のようなM平面ができる．

M平面は，M系列と同様，その自己相関関数に著しい特徴がある．式(6)のηを用い，周期(n_1, n_2)の二次元系列$\{s_{ij}\}$に対して

$$P(k, l) = \left[\sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} \eta(s_{ij})\,\eta(s_{i+k, j+l})\right] / n_1 n_2 \qquad (22)$$

で自己相関関数を定義すれば，M平面の自己相関関数は

$$P(k, l) = \begin{cases} 1 & ; (k, l) = (h_1 n_1, h_2 n_2)\ (h_1, h_2 : \text{整数}) \\ -1/n_1 n_2 & ; \text{その他の場合} \end{cases} \qquad (23)$$

となることが導ける．

M平面の一般化およびその詳しい性質については，文献(10)～(13)を参照されたい．

文 献

符号理論全般に関するもの

(1) W. W. Peterson, "Error-Correcting Codes," M. I. T. Press, Cambridge, Mass., 1961.

(2) W. W. Peterson and E. J. Weldon, "Error-Correcting Codes," 2nd Edition, M. I. T. Press, 1972.

(3) E. R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill Book Co., New York, 1968.

(4) S. Lin, "An Introduction to Error-Correcting Codes," Prentice-Hall, Inc., Englewood Cliffs, N. J., 1970.

(5) 宮川, 岩垂, 今井, "符号理論" 昭晃堂.

二次元符号に関するもの

(6) 野村, 福田, "線形再帰平面と二次元巡回符号," 信学論(A), vol. 54-A, pp. 147-154, 昭和46年3月.

(7) B. Elspas, "A Note on Multidimensional Coding," presented at the IEEE Int. Symp. Inform. Theory, San Remo, Italy, Sept. 1967.

(8) 今井, "二次元バースト訂正符号," 信学論(A), vol. 55-A, pp. 385-392, 昭和47年8月.

(9) H. Imai, "Two-Dimensional Fire Codes," submitted to IEEE Trans. Inform. Theory.

(10) 野村, 宮川, 今井, 福田, "最大面積行列をもつ平面の構成法および諸性質," 信学論(A), vol. 54-A, pp. 250-257, 昭和46年5月.

(11) ———————, "$\gamma\beta$-平面の諸性質と三次元への拡張," 信学論(A), vol. 54-A, pp. 402-409, 昭和46年7月.

(12) T. Nomura, H. Miyakawa, H. Imai and A. Fukuda, "A Theory of Two-Dimensional Linear Recurring Arrays," IEEE Trans. Inform. Theory, vol. IT-18, pp. 775-785, Nov. 1972.

(13) 中村, 岩垂, "$\gamma\beta$-平面に関する一考察," 信学会全国大会, 1156, 昭和48年3月.